IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES	:	
	:	**CRIMINAL ACTION**
v.	:	
	:	**No. 08-26**
REGINA TOLLIVER	:	

MEMORANDUM

Schiller, J. **July 29, 2009**

Defendant Regina Tolliver, a former customer service representative at the King of Prussia Mall branch of Citizens Bank, moves this Court for judgment of acquittal or, alternatively, for a new trial following convictions for bank fraud, aggravated identity theft, and unauthorized access of a financial record. Defendant's employee number and password were used in connection with a check cashing scheme. At trial, Defendant did not dispute that the bank fraud occurred, but argued that someone else used her employee number and password to acquire the customer information that allowed this scheme to flourish.

In her post trial motions, Defendant asserts that the fact that her employee number and password were used to access account information is insufficient to sustain her guilt beyond a reasonable doubt. Defendant also asserts that she is entitled to a new trial because the Government improperly shifted the burden of proof to her. For the following reasons, Defendant's motions are denied.

I. BACKGROUND

An investigation revealed that several false checks were cashed against the accounts of seven Citizens Bank customers between March and November of 2007. (Mar. 23, 2009 Tr. at 53-82;

Gov't's Exs. 102, 103, 105-09, 111-12 [Sarah Migden False Checks] & Exs. 202-04A, 206-07 [Mary Renzi False Checks] & Exs. 302-04, 306-07, 309-11, 313-14 [Lisa Parise False Checks] & Exs. 402-03, 405-06 [Veronica Tucker False Checks] & Exs 502-03, 505-06, 508, 510-11, 513, 515-16, 518, 520-21 [William Guzman False Checks] & Exs. 602-03, 605-06, 608-09 [Steven Mansh False Checks] & Exs. 702-09, 711-12, 714-16 [Evelyn Becker False Checks].) Images from Citizens Bank video cameras revealed that all of these checks were cashed by two "check runners," a male and a female, posing as the Citizens Bank account holders. (Gov't's Ex. 101, 104, 107, 110, 201, 205, 301, 305, 308, 312, 401, 404, 501, 504, 507, 509, 512, 514, 517, 519, 601, 604, 607, 701, 710, 713 [Stills of Check Runners from Citizens Bank Video].)

All of these false checks were foreign checks, meaning that they were drawn on a bank other than Citizens Bank. Once the foreign banks refused to pay, the customers were charged the face value of the checks. (*See* Mar. 23, 2009 Tr. at 58-59; *see, e.g.*, Gov't's Ex. 102A [Returned Check with Stamp].) However, since the customers were ultimately determined to be victims of fraud, Citizens Bank credited their accounts for the full value of the loss. (Mar. 23, 2009 Tr. at 59.) The false checks amounted to $181,577.00. (*Id.* at 82, 85-86; Gov't's Ex. 6 [Summ. of Fraudulent Transactions].) Thus, as a result of the fraud, Citizens Bank lost this amount. (*See* Mar. 23, 2009 Tr. at 61.)

Todd Swoyer, the fraud investigator at Citizens Bank assigned to this case, testified about the computer systems Citizens Bank utilized at the time of the fraud to manage and track its customer accounts. The systems contained customers' personal information, including names, addresses, dates of birth, social security numbers, driver's license numbers, Citizens Bank account numbers and the amount of money in those accounts. (*Id.* at 31.) Bank employees could access this

information through two systems — the main frame system and the touch point system — by entering their employee number and password.[1] (*Id.* at 31-33, 125.)

Each Citizens Bank employee is assigned an employee number, which is not confidential. (*Id.* at 124.) The password is selected by the individual employee. (*Id.* at 33.) Citizens Bank employees are instructed that their password must be kept secure and confidential and should not be written down. (*Id.* at 34; Mar. 24, 2009 Tr. at 24, 29, 33, 37-38, 43-44, 59-60.) Employees are not permitted to share their passwords with anyone else, including other Citizens Bank employees. (Mar. 23, 2009 Tr. at 34, 155.) If an employee believes that another person has learned his or her password, the employee is required to inform management and change the password immediately. (*Id.* at 34, 155-56.) If an employee must leave a terminal that she has signed into, even if just to go to the bathroom, the employee is required to temporarily lock the terminal or sign off completely. (*Id.* at 156.) Employees use their passwords frequently, between ten and fifty times daily. (Mar. 24, 2009 Tr. at 24, 30, 34, 38, 44, 60.) Additionally, Citizens Bank employees are required to change their password every two to three months. (Mar. 23, 2009 Tr. at 33.)

When a Citizens Bank employee accesses either system, data concerning that activity is archived into an employee tracking system for six months. (*Id.* at 36.) This data can be recalled to determine the employee number and password entered to access certain accounts. (*Id.*) This is known as the employee's "footprint." (*Id.*)

As part of his investigation in this case, Swoyer ran a footprint report for each of the accounts

---

[1] An employee might check both systems because, occasionally, the main frame system contained information that was not in the touch point system. (Mar. 23, 2009 Tr. at 157-58.) The account information in this case was mainly accessed via the touch point system, but was also accessed via the main frame system.

that had been compromised. (*Id.* at 87.) Swoyer's investigation revealed that Defendant's employee number was the only common employee number that had accessed these seven individuals' account information. (*Id.* at 121; Gov't's Exs. 4, 5, 114, 209, 316, 410, 531, 614, 616, 718 [Swoyer's Footprint Searches].) Swoyer's searches also revealed that, with one exception, after the account information was looked up, someone called the Citizens Bank automated system to check the balances of those accounts either shortly after the accounts were accessed or shortly before the fraudulent checks were cashed against the accounts. (Mar. 23, 2009 Tr. at 94-95; Gov't's Ex. 114, 209, 316, 410, 531, 614, 616, 718.) All of the victims who testified stated that they had not made those calls. (Mar. 23, 2009 Tr. at 214; Mar. 24, 2009 Tr. at 11, 19-21, 65.)

The Citizens Bank branch at the King of Prussia Mall maintained several universal computer terminals, which any employee could log onto using his or her employee number and password. (*Id.* at 144.) Swoyer's investigation revealed that the seven customers' accounts were accessed under Defendant's employee number on February 5th and 8th of 2007 and on March 7th, 8th, and 9th of 2007. The Citizens Bank information technology service was able to determine that the first accounts that were hit were accessed from the King of Prussia Mall branch, where Defendant worked. (*Id.* at 118; Mar. 24, 2009 Tr. at 49; Gov't's Ex. 2 [Spreadsheet] & Ex. 10.) Defendant's employee number was in use at three different terminals at the same time on that day. (Mar. 23, 2009 Tr. at 133; Mar. 24, 2009 Tr. at 51-53.) However, it was not uncommon for an employee to be logged into multiple terminals at once. (Mar. 23, 2009 Tr. at 157.)

Employee schedules and time and attendance records revealed that Defendant worked on all of the days that her password was used to access the victims' accounts. (Gov't's Ex. 10 [Employee Schedule] & Ex. 10A [Time and Attendance Records].) Defendant's employee log book for those

dates reflected that she had not contacted any of the seven victims for sales or business purposes. (Mar. 23, 2009 Tr. at 160, 163; Gov't's Ex. 12A [Def.'s Log Book].) Nor was Defendant assigned to contact any of these individuals for sales purposes. (Mar. 23, 2009 Tr. at 173-74.) Palma Salvucci, the branch manager in 2007, testified that Citizens Bank employees would not be permitted to look at a customer's account and personal information for a reason other than one related to Citizens Bank's business. (*Id.* at 165.)

According to the schedules, the only other employees at the King of Prussia Mall branch who arguably worked on the relevant days were Angela Anderson and Debby Clarke. Clarke was initially marked as "OFF" for Febraury 8th, March 7th, and March 8th, but the notation "KOP" was written next to her slot on those dates. Salvucci, who assembled the schedules, testified that she used this notation when asked to lend an employee for the day to the other Citizens Bank branch in King of Prussia and that she would change it if she received a call not to send the employee. (*Id.* at 152.) However, she testified that it is not possible to know for sure, based only on the schedule, whether an individual marked as working at the other Citizens Bank branch for the day in fact did so. (*Id.* at 153.) Indeed, although the "KOP" notation appeared next to Clarke's schedule for March 7th and 8th, the time and attendance records reflect that she did not work at all on those days.[2] (Gov't's Ex. 10A.)

Swoyer and Postal Inspector Frank Busch interviewed Defendant on March 15, 2007. (Mar. 23, 2009 Tr. at 122, 196.) Defendant told Swoyer that she had not given her password to anyone,

[2] The "KOP" notation was written on Defendant's schedule for February 8, 2007. (Gov't's Ex. 10.) The time and attendance records reflect that, whether she worked at the King of Prussia Mall branch or the other Citizens Bank branch in King of Prussia, Defendant worked on that day. (Gov't's Ex. 10A.) There was no evidence at trial identifying the branch that the victims' accounts were accessed from on February 8, 2007.

and stated that she always locked her computer when she walked away from a terminal. (*Id.* at 122) Additionally, all of Defendant's former co-workers who testified at trial claimed that they never knew Defendant's password and that they never saw her password written down. (*Id.* at 156; Mar. 24, 2009 Tr. at 25, 30-31, 34-35, 39, 44-45, 60.) Although a page in Defendant's log book read "password, Aries12, as HR express, password, evil1ass, lifecare, RSM1love, Aries12," Defendant told Swoyer that these were not her passwords to access the touch point or the main frame systems. (Mar. 23, 2009 Tr. at 137.) Defendant was terminated that day. (*Id.* at 131.)

The Government theorized that Defendant accessed customers' personal and account information and passed this information along for use in a scheme to defraud Citizens Bank. Ultimately, the information was used to create false identification documents, which were used by the check runners to cash fraudulent checks against the targeted accounts. However, neither of the check runners in this case, both of whom had been arrested, implicated Defendant. (*Id.* at 198.)

Busch, the Government's expert on financial crimes, testified about the structure of bank fraud schemes. (*Id.* at 175-77.) Inspector Busch testified that, generally speaking, bank fraud schemes involve the following participants: a ring leader who heads the operation; a second in command who, among other things, recruits individuals to assist in the operation; individuals who can access or create counterfeit documents; drivers who take check runners to the bank to cash the false checks; check runners who go into the bank to cash the checks; and individuals, such as employees at banks or insurance companies, who access personal information to be used in the scheme. (*Id.* at 178, 182, 187.) According to Inspector Busch, the bank employee would typically be in touch with the ring leader of the operation or the middle man who recruited her, but would not have contact with the check runners. (*Id.* at 179-81.) Thus, in his experience, check runners

generally do not know the identity of the person who is obtaining the information to facilitate the crime. (*Id.* at 183-84.)

Inspector Busch also explained that, in general, a bank employee will access personal information, write it down or print it out, and then pass it along to be used in the scheme. (*Id.* at 189.) It is common, as was the case here, for someone in the scheme to call the automated system to confirm that the targeted accounts are active and functioning properly. (*Id.* at 190.)

II. STANDARD OF REVIEW

When considering a claim that the evidence at trial was insufficient to support a conviction pursuant to Federal Rule of Criminal Procedure 29, a district court views the evidence "in the light most favorable to the government and affirm[s] the judgment if there is substantial evidence from which any rational trier of fact could find [the defendant] guilt[y] beyond a reasonable doubt." *United States v. Frorup*, 963 F.2d 41, 42 (3d Cir. 1992); *see also United States v. Gambone*, 314 F.3d 163, 170 (3d Cir. 2003); FED. R. CRIM. P. 29. A court must "credit all available inferences in favor of the government." *United States v. Riddick*, 156 F.3d 505, 509 (3d Cir. 1998). If evidence emerges from the trial that supports the jury's verdict, regardless of how probative the court believes it to be, then a defendant's motion for acquittal based on insufficient evidence should be denied. *See United States v. McNeill*, 887 F.2d 448, 450 (3d Cir. 1989). "The 'contention that the evidence also permits a less sinister conclusion is immaterial. To sustain the jury's verdict, the evidence does not need to be inconsistent with every conclusion save that of guilt.'" *United States v. Smith*, 294 F.3d 473, 478 (3d Cir. 2002) (quoting *United States v. Dent*, 149 F.3d 180, 188 (3d Cir. 1998)).

Pursuant to Federal Rule of Criminal Procedure 33, a court may grant a new trial "if the

interest of justice so requires." FED. R. CRIM. P. 33(a). A district court has discretion to "grant a defendant a new trial only if it finds that 'there is a serious danger that a miscarriage of justice has occurred — that is, that an innocent person has been convicted.'" *United States v. Rich*, 326 F. Supp. 2d 670, 673 (E.D. Pa. 2004) (quoting *United States v. Johnson*, 302 F.3d 139, 150 (3d Cir. 2002)). Although this standard is broader than the standard for acquittal under Rule 29, motions for a new trial are disfavored and "only granted with great caution and at the discretion of the trial court." *United States v. Martinez*, 69 F. App'x 513, 516 (3d Cir. 2003).

III. DISCUSSION

A. Defendant is not Entitled to Judgment of Acquittal

To establish that Defendant was guilty of bank fraud, the Government was required to establish that Defendant "knowingly execute[d], or attempt[ed] to execute a scheme or artifice (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations or promises." 18 U.S.C. § 1344. "[W]here the bank is a direct target of the deceptive conduct or scheme, § 1344 is satisfied by proof of a specific intent to defraud the bank plus fraudulent conduct (e.g., misrepresentations) which creates an actual loss or risk of loss." *United States v. Leahy*, 445 F.3d 634, 646 (3d Cir. 2006); *see also United States v. Thomas*, 315 F.3d 190, 197 (3d Cir. 2002). Defendant's convictions for aggravated identity theft must be sustained if the Government has proved that she "knowingly transfer[red], possesse[d], or use[d], without lawful authority, a means of identification of another person" during the commission of bank fraud. 18 U.S.C. § 1028A(a)(1), (c). To prove Defendant guilty of unauthorized access of

a financial record, the Government was required to establish that she "intentionally accesse[d] a computer without authorization or exceed[ed] authorized access, and thereby obtain[ed] . . . information contained in a financial record of a financial institution." 18 U.S.C. § 1030(a)(2)(A) (2008). The legislative history of this section makes clear that "'obtaining information' in this context includes mere observation of the data." S. REP. NO. 99-432 at 2484 (1986). "Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of [subsection 1030(a)(2)]." *Id.*

Defendant was also charged with aiding and abetting bank fraud and aggravated identity theft. "In order to convict a defendant of aiding and abetting the commission of a crime the government must prove: (1) that the substantive crime has been committed; and (2) that the defendant charged with aiding and abetting knew of the commission of the substantive offense and acted with the intent to facilitate it." *United States v. Soto*, 539 F.3d 191, 194 (3d Cir. 2008). Aiding and abetting can be established solely by circumstantial evidence. *Id.*

The Government unquestionably established that false checks in the amount of $181,577.00 were cashed against the accounts of seven Citizens Bank customers as part of a scheme to defraud Citizens Bank and that Citizens Bank sustained a loss in that amount. The Government also established that someone used Defendant's employee number and password to access the account and personal information of these seven individuals and that Defendant's employee number was the only employee number used in relation to all seven accounts. The timing of the access of those accounts relative to the inquiries into the Citizens Bank automated system and subsequent cashing of false checks supports the conclusion that someone used Defendant's employee number and password with the intent to further the scheme to defraud the bank. The key question is whether

there was sufficient evidence at trial to establish that it was Defendant who used her password on the dates in question to access information in furtherance of this scheme.

The Government provided circumstantial evidence that it was Defendant, and not another person using Defendant's password, who accessed the account information in the Citizens Bank system. Evidence at trial showed that Citizens Bank employees select their own passwords, are instructed to keep their passwords secret and are prohibited from sharing them with other employees or writing them down. Defendant herself told Mr. Swoyer and Inspector Busch that she safeguarded her password and that she had not given it to anyone else. Furthermore, all of Defendant's former co-workers who testified at trial stated that they did not know Defendant's password. There was also evidence that Defendant worked on each of the days that the victims' accounts were accessed with her password and evidence that there was no legitimate business purpose for her to access those accounts.

Based on this evidence, a reasonable jury could infer that only Defendant knew her password and that it was she who entered her password into the system. The possibility that Defendant's password was compromised is an insufficient basis to grant Defendant judgment of acquittal. No evidence was introduced in support of this theory and the jury was not required to accept such a conclusion since it was reasonable to infer that Defendant was the culprit. *See United States v. Shea*, 493 F.3d 1110, 1117-18 (9th Cir. 2007) (that other employees "had access to [defendant's] computer or could have logged on as him remotely" did not warrant acquittal of computer-related offenses where defendant had access to files that corrupted data on computer and his user name and password were associated with the file). The jury was also entitled to credit Inspector Busch's testimony to conclude that the check runners did not implicate Defendant because they would not have had

contact with her given their respective roles in the scheme. Viewing the evidence in a light most favorable to the Government, sufficient evidence supports the conclusion that Defendant committed the charged offenses. Accordingly, Defendant is not entitled to judgment of acquittal.

Defendant also argues that she is entitled to acquittal because the Government failed to establish that she "[had] custody and control over a particular computer only available to her in addition to her ID appearing on the computer log sheets." (Def.'s Mem. in Supp. of Mot. for J. of Acquittal and or New Trial [hereinafter Def.'s Mem.] at 3.) There is no requirement that the Government prove that Defendant had exclusive custody and control over the computers used to commit the charged offenses, only a requirement that the Government prove its case beyond a reasonable doubt. *See Shea*, 493 F.3d at 1116 (sufficient evidence sustained convictions for computer tampering offenses even though "user names and passwords were not tied to each other, or to any given machine"). It is undisputed that Defendant had access to the Citizens Bank computers. That other employees also had access to those same computers is irrelevant if none of them knew nor had access to Defendant's password. Without Defendant's password, none of the other employees could have accessed the accounts under her name. The jury clearly credited the testimony of Defendant's former co-workers that they did not know her password and this Court may not second guess this rational conclusion. Likewise, that "[t]here was no allegation or evidence presented at trial that the defendant prepared any phony identifications of the Citizens Bank customers or helped obtain the bogus checks" (Def.'s Post Trial Mots. at 3) does not warrant acquittal since Defendant's use of her position as a Citizens Bank employee to acquire customers' personal information to facilitate fraud establishes that she aided and abetted bank fraud and aggravated identity theft.

Defendant also argues that she is entitled to acquittal because the Government "failed to show what information was accessed and who it was allegedly passed onto." (Def.'s Mem. at 2.) First, the Government did, in fact, establish what information was accessed. The codes that appeared on the footprint for Defendant's employee number revealed that she looked up personal information in the Citizens Bank system, including names, social security numbers and account information. (Mar. 23, 2009 Tr. at 31, 35-50, 92-114.) Second, although the Government did not identify the individuals to whom the information was passed, the Government was not required to do so to carry its burden of proof. *See United States v. Wasserson*, 418 F.3d 225, 233 (3d Cir. 2005) ("It is not a prerequisite to the conviction of the aider and abettor that the principal be tried and convicted or in fact even be identified.") (quoting *United States v. Provenzano*, 334 F.2d 678, 691 (3d Cir. 1964)).

Defendant also asserts that "[from] [t]he fact that an alleged access was unauthorized [it] does not follow that said access was a crime." (Def.'s Mem. at 3.) The evidence at trial indicated that there was no legitimate business reason for Defendant to access these customers' accounts. Salvucci testified that Citizens Bank employees were not permitted to access customer information without a legitimate business purpose. Since Defendant accessed the customers' personal and account information via the Citizens Bank system, which constitutes "information contained in a financial record of a financial institution" within the meaning of 18 U.S.C. § 1030, and since she exceeded her authorized access in doing so, her conviction under that statute is appropriate. *See* 18 U.S.C. § 1030(e)(4)(A) (defining "financial institution" to include "an institution, with deposits insured by the Federal Deposit Insurance Corporation"); *id.* § 1030(e)(5) (defining "financial record" as "information derived from any record held by a financial institution pertaining to a customer's

relationship with the financial institution").[3]

Additionally, there is overwhelming evidence that the information was used to perpetrate a fraud on Citizens Bank. The jury was entitled to credit Inspector Busch's testimony concerning the innerworkings of bank fraud schemes to conclude that Defendant passed the information to someone else in the scheme. Shortly after Defendant accessed the first three accounts, someone other than the account holder checked the balance to ensure that the account was still active and that sufficient funds existed to cover the amount of the false checks to be cashed against them. Then, check runners cashed several false checks against those accounts, resulting in payouts of thousands of dollars. Thus, the jury could infer that Defendant accessed these accounts because she was involved in a scheme to defraud the bank and that she passed the account information along to other members of the scheme to further that objective. This makes her unauthorized access a crime — aiding and abetting bank fraud and aggravated identity theft.

Defendant also complains that the Government did not establish that the accessed information was recorded or possessed by Defendant. The Government need not establish that the information accessed from the Citizens Bank system was "recorded" or "possessed" but merely that: (1) it was "obtained," for purposes of sustaining Defendant's § 1030 conviction; (2) that it was "knowingly transfer[red], possesse[d], or use[d], without lawful authority" during the commission of bank fraud, for purposes of sustaining Defendant's convictions for aggravated identity theft or aiding and abetting; and (3) that Defendant accessed this information in furtherance of a scheme to defraud Citizens Bank, for purposes of sustaining her bank fraud conviction. As discussed above,

[3] The parties stipulated that Citizens Bank was insured by the Federal Deposit Insurance Corporation when the fraud occurred.

the Government proved its case beyond a reasonable doubt and thus this Court will not grant Defendant's motion for judgment of acquittal.

B. Defendant is not Entitled to a New Trial

Defendant asserts that she is entitled to a new trial because the Government focused on "the defendant's lack of a[n] explanation or evidence" to prove its case, thereby "violat[ing] the defendant's constitutional right to remain silent and unconstitutionally shift[ing] the burden of proof upon defendant." (Def.'s Mem. at 5.) Defendant does not identify any particular statement made by the Prosecutor nor does she cite any law in support of her argument.

Defendant made no objection to the Government's opening or closing at trial. Regardless, no constitutional violation occurred here because the Government's arguments appropriately summarized the evidence in the case. Certainly, a prosecutor "may not comment on a defendant's failure to testify and may not improperly suggest that the defendant has the burden to produce evidence." *United States v. Balter*, 91 F.3d 427, 441 (3d Cir. 1996). However, a prosecutor, in attempting to prove her case, may point to the absence of evidence supporting the Defendant's theory of the crime. *Id.* (prosecutor's comment merely "attempted to focus the jury's attention on holes in the defense's theory"); *see also United States v. Lore*, 430 F.3d 190, 213 (3d Cir. 2005).

In its closing and rebuttal, the Government highlighted the circumstantial evidence suggesting that it was Defendant, and not another individual, who used her employee number and password to access the compromised accounts. The prosecutor summarized the instructions given to Citizens Bank employees to safeguard their passwords and reminded the jury that the employees themselves selected these passwords and used them numerous times during the course of the work day. The prosecutor also noted that Defendant's former co-workers testified that they did not know

Defendant's password. After Defense Counsel's attempt to raise reasonable doubt in his closing by suggesting that Defendant's password was compromised, the Prosecutor stated in her rebuttal that:

> You also heard [Defense Counsel] say that passwords are compromised all the time. There is no evidence being presented to you of passwords being compromised all the time. The only evidence you've heard is about the employees who came in here and talked about their passwords and what they do to protect them, and how they behave and how they operate in their work place.

(Mar. 24, 2009 Tr. at 117-18.) There is nothing improper about this statement, which merely summarized the evidence presented; nor did the Government make any other statements that improperly shifted the burden of proof to Defendant or commented on Defendant's failure to testify. Accordingly, a new trial is not warranted on this basis.

IV. CONCLUSION

There was sufficient evidence at trial for a jury to conclude that Defendant accessed the account information of Citizens Bank customers to defraud the bank. Accordingly, Defendant's motion for judgment of acquittal is denied. Defendant's motion for a new trial is also denied. An appropriate Order will be docketed with this Memorandum.